COMMISSION IMPLEMENTING DECISION

of XXX

pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Article 25(6) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

1. Introduction

(1) Directive 95/46/EC sets the rules for transfers of personal data from Member States to third countries to the extent that such transfers fall within its scope.

(2) Article 1 of Directive 95/46/EC and recitals 2 and 10 in its preamble seek to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms.[2]

(3) The importance of both the fundamental right to respect for private life, guaranteed by Article 7, and the fundamental right to the protection of personal data, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, has been emphasised in the case-law of the Court of Justice.[3]

(4) Pursuant to Article 25(1) of Directive 95/46/EC Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and the Member State laws implementing other provisions of the Directive are respected prior to the transfer. The Commission may find that a third country ensures such an adequate level of protection

[1] OJ L 281, 23.11.1995, p. 31.

[2] Case C-362/13, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems*"), EU:C:2015:650, paragraph 39.

[3] Case C-553/07, *Rijkeboer*, EU:C:2009:293, paragraph 47; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, paragraph 53; Case C-131/12, *Google Spain and Google*, EU:C:2014:317, paragraphs 53, 66 and 74.

by reason of its domestic law or of the international commitments it has entered into in order to protect the rights of individuals. In that case, and without prejudice to compliance with the national provisions adopted pursuant to other provisions of the Directive, personal data may be transferred from the Member States without additional guarantees being necessary.

(5) Pursuant to Article 25(2) of Directive 95/46/EC, the level of data protection afforded by a third country should be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations, including the rules of law, both general and sectorial, in force in the third country in question.

(6) In Commission Decision 520/2000/EC[4], for the purposes of Article 25(2) of Directive 95/46/EC, the "Safe Harbour Privacy Principles", implemented in accordance with the guidance provided by the so-called "Frequently Asked Questions" issued by the U.S. Department of Commerce, were considered to ensure an adequate level of protection for personal data transferred from the Union to organisations established in the United States.

(7) In its Communications COM(2013) 846 final[5] and COM(2013) 847 final of 27 November 2013[6], the Commission considered that the fundamental basis of the Safe Harbour scheme had to be reviewed and strengthened in the context of a number of factors, including the exponential increase in data flows and their critical importance for the transatlantic economy, the rapid growth of the number of U.S. companies adhering to the Safe Harbour scheme and new information on the scale and scope of certain U.S. intelligence programs which raised questions as to the level of protection it could guarantee. In addition, the Commission identified a number of shortcomings and deficiencies in the Safe Harbour scheme.

(8) Based on evidence gathered by the Commission, including information stemming from the work of the EU-US Privacy Contact Group[7] and the information on US intelligence programs received in the ad hoc EU-US Working Group[8], the Commission formulated 13 recommendations for a review of the Safe Harbour scheme. These recommendations focused on strengthening the substantive privacy principles, increasing the transparency of U.S. self-certified companies' privacy policies, better supervision, monitoring and enforcement by the U.S. authorities of compliance with those principles, the availability of affordable dispute resolution mechanisms, and the need to ensure that use of the national security exception

---

4 Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (OJ L 215 of 28.8.2000, p. 7).

5 Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-U.S. Data Flows, COM(2013) 846 final of 27.11.2013.

6 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final of 27.11.2013.

7 See e.g. Council of the European Union, Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, Note 9831/08, 28 May 2008, available on the internet at: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

8 Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27.11.2013, available on the internet at: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

foreseen in Commission Decision 520/2000/EC is limited to an extent that is strictly necessary and proportionate.

(9) In its judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*[9], the Court of Justice of the European Union declared Commission Decision 520/2000/EC invalid. Without examining the content of the Safe Harbour Privacy Principles, the Court considered that the Commission had not stated in that decision that the United States in fact 'ensured' an adequate level of protection by reason of its domestic law or its international commitments.[10]

(10) In this regard, the Court of Justice explained that, while the term 'adequate level of protection' in Article 25(6) of Directive 95/46/EC does not mean a level of protection identical to that guaranteed in the EU legal order, it must be understood as requiring the third country to ensure a level of protection of fundamental rights and freedoms 'essentially equivalent' to that guaranteed within the Union by virtue of Directive 95/46/EC read in the light of the Charter of Fundamental Rights. Even though the means to which that third country has recourse, in this connection, may differ from the ones employed within the Union, those means must nevertheless prove, in practice, effective.[11]

(11) The Court of Justice criticised the lack of sufficient findings in Decision 2000/520/EC regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and the existence of effective legal protection against interference of that kind.[12]

(12) In 2014 the Commission had entered into talks with the U.S. authorities in order to discuss the strengthening of the Safe Harbour scheme in line with the 13 recommendations contained in Communication COM(2013) 847 final. After the judgment of the Court of Justice of the European Union in the *Schrems* case, these talks were intensified, in order to come to a new adequacy decision which would meet the requirements of Article 25 of Directive 95/46/EC as interpreted by the Court of Justice. The documents which are annexed to this decision and will also be published in the U.S. Federal Register are the result of these discussions. The Privacy Principles (Annex II), together with the official representations and commitments by various U.S. authorities contained in the documents in Annexes I, III to VII, constitute the "EU-U.S. Privacy Shield".

(13) The Commission has carefully analysed U.S. law and practice, including these official representations and commitments. Based on the findings developed in recitals (112)-(116), the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.

[9] See footnote 2.
[10] *Schrems*, paragraph 97.
[11] *Schrems*, paragraphs 73-74.
[12] *Schrems*, paragraph 88-89.

2. The "EU-U.S. Privacy Shield"

(14) The EU-U.S. Privacy Shield is based on a system of self-certification by which U.S. organisations commit to a set of privacy principles – the EU-U.S. Privacy Shield Framework Principles, including the Supplemental Principles (hereinafter together: "the Privacy Principles") – issued by the U.S. Department of Commerce and contained in Annex II to this decision.

(15) This system will be administered by the Department of Commerce based on its commitments set out in the representations from the U.S. Secretary of Commerce (Annex I to this decision). With regard to the enforcement of the Privacy Principles, the Federal Trade Commission (FTC) and the Department of Transportation have made representations that are contained in Annex IV and Annex V to this decision.

2.1. Privacy Principles

(16) As part of their self-certification under the EU-U.S. Privacy Shield, organisations have to commit to comply with the Privacy Principles.[13]

(17) Under the *Notice Principle*, organisations are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data (e.g. type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability). Further safeguards apply, in particular the requirement for organisations to make public their privacy policies (reflecting the Privacy Principles) and to provide links to the Department of Commerce's website (with further details on self-certification, the rights of data subjects and available recourse mechanisms), the Privacy Shield List referred to in recital (24) and the website of an appropriate alternative dispute settlement provider.

(18) Under the *Choice Principle*, data subjects may object (opt out) if their personal data shall be disclosed to a third party (other than an agent acting on behalf of the organisation) or used for a "materially different" purpose. In case of sensitive data, organisations must in principle obtain the data subject's affirmative express consent (opt in). Moreover, under the Choice Principle, special rules for direct marketing generally allowing for opting out "at any time" from the use of personal data apply.

(19) Under the *Security Principle*, organisations creating, maintaining, using or disseminating personal data must take "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the data. In the case of sub-processing, organisations must conclude a contract with the sub-processor guaranteeing the same level of protection as provided by the Privacy Principles and take steps to ensure its proper implementation.

(20) Under the *Data Integrity and Purpose Limitation Principle*, personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended

[13] Special rules providing additional safeguards apply for human resources data collected in the employment context as laid down in the supplemental principle on "Human Resources Data" of the Privacy Principles. For instance, employers should accommodate the privacy preferences of employees by restricting access to the personal data, anonymising certain data or assigning codes or pseudonyms. Most importantly, organisations are required to cooperate and comply with the advice of Union Data Protection Authorities when it comes to such data.

use, accurate, complete and current. An organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject.

(21) Under the *Access Principle*, data subjects have the right, without need for justification and only against a non-excessive fee, to obtain from an organisation confirmation of whether such organisation is processing personal data related to them and have the data communicated within reasonable time. This right may only be restricted in exceptional circumstances; any denial of, or limitation to the right of access has to be necessary and duly justified, with the organisation bearing the burden of demonstrating that these requirements are fulfilled. Data subjects must be able to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Privacy Principles.

(22) Under the *Accountability for Onward Transfer Principle*, any onward transfer of personal data from an organisation to controllers or processors can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group) and (iii) only if that contract provides the same level of protection as the one guaranteed by the Privacy Principles. This should be read in conjunction with the *Notice* and especially with the *Choice Principle*, according to which data subjects can object (opt out) or, in the case of sensitive data, have to give "affirmative express consent" (opt in) for onward transfers. Where compliance problems arise in the (sub-) processing chain, the organisation acting as the controller of the personal data will have to prove that it is not responsible for the event giving rise to the damage, or otherwise face liability.

(23) Finally, under the *Recourse, Enforcement and Liability Principle*, participating organisations must provide robust mechanisms to ensure compliance with the other Privacy Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies. Once an organisation has voluntarily decided to self-certify under the EU-U.S. Privacy Shield, its effective compliance with the Privacy Principles is compulsory. To be allowed to continue to rely on the Privacy Shield to receive personal data from the Union, such organisation must annually re-certify its participation in the framework. Also, organisations must take measures to verify that their published privacy policies conform to the Privacy Principles and are in fact complied with. This can be done either through a system of self-assessment, which must include internal procedures ensuring that employees receive training on the implementation of the organisation's privacy policies and that compliance is periodically reviewed in an objective manner, or outside compliance reviews, the methods of which may include auditing or random checks. In addition, the organisation must put in place an effective redress mechanism to deal with such complaints (see in this respect also recital (30).

2.2. Transparency and Administration of the EU-U.S. Privacy Shield

(24) To ensure the proper application of the EU-U.S. Privacy Shield, it is necessary that organisations adhering to the Privacy Principles can be identified as such by interested parties, such as data subjects, data exporters and the national Data Protection Authorities ("DPAs"). To this end, the Department of Commerce (or its designee) has undertaken to maintain and make available to the public a list of organisations that have self-certified their adherence to the Privacy Principles and fall within the

jurisdiction of at least one of the government bodies mentioned in Annexes I, II to this decision ("Privacy Shield List"). The Department of Commerce will update the list on the basis of annual re-certification submissions and whenever an organisation withdraws or is removed from the EU-U.S. Privacy Shield. It will also maintain and make available to the public an authoritative record of organisations that have been removed from the list, in each case identifying the reason for such removal. Finally, it will provide a link to the list of Privacy Shield-related FTC cases maintained on the FTC website.

(25) Both the Privacy Shield List and the re-certification submissions will be made publicly available through the Department of Commerce's dedicated website and self-certified organisations must provide the web address for the Privacy Shield List. In addition, if available online, an organisation's privacy policy must include a hyperlink to the Privacy Shield website as well as a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.

(26) Organisations that have persistently failed to comply with the Privacy Principles will be removed from the Privacy Shield List and must return or delete the personal data received under the EU-U.S. Privacy Shield. In other cases of removal, the organisation may retain such data if it affirms to the Department of Commerce on an annual basis its commitment to continue to apply the Principles or provides adequate protection for the personal data by another authorised means (e.g. by using a contract that fully reflects the requirements of the relevant standard contractual clauses approved by the Commission). In this case, an organisation has to identify a contact point within the organisation for all Privacy Shield-related questions.

(27) When an organisation leaves the EU-U.S. Privacy Shield for any reason, it must remove all public statements implying that it continues to participate in the EU-U.S. Privacy Shield or is entitled to its benefits, in particular any references to the EU-U.S. Privacy Shield in its published privacy policy. Any misrepresentation to the general public concerning an organisation's adherence to the Privacy Principles in the form of misleading statements or practices is enforceable by the FTC, Department of Transportation or other relevant U.S. enforcement authorities; misrepresentations to the Department of Commerce are enforceable under the False Statements Act (18 U.S.C. § 1001).

(28) The Department of Commerce will *ex officio* monitor any false claims of Privacy Shield participation or the improper use of the Privacy Shield certification mark, and DPAs can refer organisations for review to a dedicated contact point at the Department. When an organisation has withdrawn from the EU-U.S. Privacy Shield, fails to re-certify or is removed from the Privacy Shield List, the Department of Commerce will on an on-going basis verify that it has deleted from its published privacy policy any references to the Privacy Shield that imply its continued participation and, if it continues to make false claims, refer the matter to the FTC, Department of Transportation or other competent authority for possible enforcement action. It will also send questionnaires to organisations whose self-certifications lapse or that have voluntarily withdrawn from the EU-U.S. Privacy Shield to verify whether the organisation will return, delete or continue to apply the Privacy Principles to the personal data that they received while participating in the EU-U.S. Privacy Shield and, if personal data are to be retained, verify who within the organisation will serve as an ongoing contact point for Privacy Shield-related questions.

2.3. Compliance review and complaint handling

(29) The EU-U.S. Privacy Shield, through the *Recourse, Enforcement and Liability Principle* and the commitments undertaken by the Department of Commerce, the FTC and the Department of Transportation, provides a number of mechanisms to ensure compliance by U.S. self-certified companies with the Privacy Principles. These include the oversight and enforcement through the Department of Commerce and independent authorities (such as the FTC and, in certain cases, the DPAs) as well as the possibility for EU data subjects to lodge complaints regarding non-compliance by U.S. self-certified companies and to have these complaints resolved, if necessary by a decision providing an effective remedy.

(30) First, EU data subjects may vindicate their rights and pursue cases of non-compliance with the Privacy Principles through direct contacts with the *U.S. self-certified company*. To facilitate resolution, the organisation must put in place an effective redress mechanism to deal with such complaints. This includes that an organisation's privacy policy must clearly inform individuals about a contact point, either within or outside the organisation, that will handle complaints (including any relevant establishment in the Union that can respond to inquiries or complaints) and about the independent complaint handling mechanisms. Upon receipt of a complaint, including through the Department of Commerce following referral by a DPA, the organisation must, within a period of 45 days, provide a response to the EU data subject. This response must provide an assessment of the merits of the complaint and, if so, information as to how the organisation will rectify the problem. Likewise, organisations are required to respond promptly to inquiries and other requests for information from the Department of Commerce (or, where the organisation has committed to cooperate with the DPAs, the handling authority designated by the panel of DPAs provided for in the supplemental principle on "The Role of the Data Protection Authorities") relating to their adherence to the Privacy Principles. Finally, organisations must retain their records on the implementation of their privacy policies and make them available upon request in the context of an investigation or a complaint about non-compliance to an independent recourse mechanism or the FTC (or other U.S. authority with jurisdiction to investigate unfair and deceptive practices).

(31) Second, organisations must designate an *independent dispute resolution body* (either in the United States or in the Union) to investigate and resolve individual complaints (unless they are obviously unfounded or frivolous) and to provide appropriate recourse free of charge to the individual. Sanctions and remedies imposed by such a body must be sufficiently rigorous to ensure compliance by organisations with the Privacy Principles and should provide for a reversal or correction by the organisation of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for findings of non-compliance. Independent dispute resolution bodies designated by an organisation will be required to include on their public websites relevant information regarding the EU-U.S. Privacy Shield and the services they provide under it. Each year, they must publish an annual report providing aggregate statistics regarding these services.[14]

[14] The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the

(32) Alternatively, where organisations opt to subscribe to private-sector developed *privacy programs* that incorporate the Privacy Principles into their rules, these must include effective enforcement mechanisms.

(33) In case the organisation fails to comply with the ruling of a dispute resolution or self-regulatory body, the latter must notify such non-compliance to the Department of Commerce and the FTC (or other U.S. authority with jurisdiction to investigate unfair and deceptive practices), or a competent court.

(34) Third, the *Department of Commerce* will systematically verify, in the context of an organisation's certification and re-certification to the framework, that its privacy policies conform to the Principles. It will maintain an updated list of participating organisations.

(35) On an ongoing basis, the Department of Commerce will conduct *ex officio* compliance reviews of self-certified organisations, including through sending detailed questionnaires. It will also systematically carry out reviews whenever it has received a specific (non-frivolous) complaint, when an organisation does not provide satisfactory responses to its enquiries, or when there is credible evidence suggesting that an organisation may not be complying with the Privacy Principles.

(36) In addition, the Department of Commerce has committed to receive, review and undertake best efforts to resolve complaints about an organisation's non-compliance with the Privacy Principles. To this end, the Department of Commerce provides special procedures for DPAs to refer complaints to a dedicated contact point, track them and follow up with companies to facilitate resolution. In order to expedite the processing of individual complaints, the contact point will liaise directly with the respective DPA on compliance issues and in particular update it on the status of complaints within a period of not more than 90 days following referral. This allows data subjects to bring complaints of non-compliance by U.S. self-certified companies directly to their national DPA and have them channelled to the Department of Commerce as the U.S. authority administering the EU-U.S. Privacy Shield. The Department of Commerce has also committed to provide, in the annual review of the functioning of the EU-U.S. Privacy Shield, a report that analyses in aggregate form the complaints it receives each year.

(37) The Department of Commerce will also verify that self-certified U.S. companies have actually registered with the independent recourse mechanisms they claim they are registered with. Both the organisations and the responsible independent recourse mechanisms are required to respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield.

(38) Where, on the basis of its *ex officio* verifications, complaints or any other information, the Department of Commerce concludes that an organisation has persistently failed to comply with the Privacy Principles it will remove such an organisation from the Privacy Shield list. Refusal to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body, including a DPA, will be regarded as a persistent failure to comply.

(39) The Department of Commerce will maintain an updated list of organisations that are no longer part of the framework, setting out the reasons for their removal from the list. In addition, it will monitor organisations that are no longer members of the EU-U.S.

length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed**.**

Privacy Shield, either because they have voluntarily withdrawn or because their certification has lapsed, to verify whether they will return, delete or retain the personal data received previously under the framework. In the latter case, organisations are obliged to continue to apply the Privacy Principles to these personal data. In cases where the Department of Commerce has removed organisations from the framework due to a persistent failure to comply with the Privacy Principles, it will ensure that those organisations must return or delete the personal data they received under the framework. Moreover, the Department of Commerce will actively search for and address false claims of participation in the framework, including by former members. Such false claims may be actionable by the FTC or other enforcement agency.

(40) Fourth, the *Federal Trade Commission* will give priority consideration to referrals of non-compliance with the Privacy Principles received from independent dispute resolution or self-regulatory bodies, the Department of Commerce and DPAs (acting on their own initiative or upon complaints) to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive practices has been violated. The FTC has committed to create a standardised referral process, to designate a point of contact at the agency for DPA referrals, and to exchange information on referrals. In addition, it will accept complaints directly from individuals and will undertake Privacy Shield investigations on its own initiative, in particular as part of its wider investigations of privacy issues.

(41) The FTC can enforce compliance through administrative orders ("consent orders"), and it will systematically monitor compliance with such orders. Where organisations fail to comply, the FTC may refer the case to the competent court in order to seek civil penalties and other remedies, including for any injury caused by the unlawful conduct. Alternatively, the FTC may directly seek a preliminary or permanent injunction or other remedies from a federal court. Each consent order issued to a Privacy Shield organisation will have self-reporting provisions[15], and organisations will be required to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC. Finally, the FTC will maintain an online list of companies subject to FTC or court orders in Privacy Shield cases.

(42) Fifth, where a national *Data Protection Authority* investigates a complaint regarding non-compliance with the Privacy Principles, organisations are obliged to cooperate in the investigation and the resolution of this complaint if it concerns processing of human resources data collected in the context of an employment relationship or if they have voluntarily submitted to the oversight by DPAs. Notably, they have to respond to inquiries, comply with the advice given by the DPA, including for remedial or compensatory measures, and provide the DPA with written confirmation that such action has been taken. In order to facilitate cooperation, the Department of Commerce will establish a dedicated contact point to act as a liaison and to assist with DPA inquiries regarding an organisation's compliance with the Privacy Principles. Likewise, the FTC has committed to provide the DPAs with investigatory assistance pursuant to the U.S. SAFE WEB Act.[16]

(43) The advice of the DPAs will be delivered through an informal panel of DPAs established at Union level, which will also help to ensure a harmonised and coherent

---

[15] FTC or court orders may require companies to implement privacy programs and to regularly make compliance reports or independent third-party assessments of those programs available to the FTC.

[16] U.S. SAFE WEB Act of 2006, Pub. L. 109-455 of 22.12.2006.

approach.[17] Advice will be issued after both sides in the dispute have had a reasonable opportunity to comment to provide any evidence they wish. The respective DPA will deliver advice as quickly as the requirement for due process allows, and as a general rule within 60 days after receiving a complaint. If an organisation fails to comply within 25 days of delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the FTC (or other competent U.S. enforcement authority), or to conclude that the commitment to cooperate has been seriously breached. In the first alternative, this may lead to enforcement action based on Section 5 of the FTC Act (or similar statute). In the second alternative, the panel will inform the Department of Commerce which will consider the organisation's refusal as a persistent failure to comply that will lead to the organisation's removal from the Privacy Shield List.

(44) Where a DPA, upon receiving a claim by an EU data subject, considers that the individual's personal data transferred to an organisation in the United States are not afforded an adequate level of protection, it can also exercise its powers vis-à-vis the data exporter and, if necessary, suspend the data transfer.

(45) In all these cases, if the DPA to which the complaint has been addressed has taken no or insufficient action to address a complaint, the individual complainant has the possibility to challenge such (in-) action in the national courts of the respective Member State.

(46) Sixth, as a recourse mechanism of 'last resort' in case none of the other available redress avenues has satisfactorily resolved an individual's complaint, the EU data subject may invoke binding arbitration by the *"Privacy Shield Panel"*. This panel will consist of a pool of at least 20 arbitrators designated by the Department of Commerce and the Commission based on their independence, integrity, as well as experience in U.S. privacy and Union data protection law. For each individual dispute, the parties will select from this pool a panel of one or three[18] arbitrators. The proceedings will be governed by standard arbitration rules to be agreed between the Department of Commerce and the Commission. While the arbitration will take place in the United States, EU data subjects may choose to participate through video or telephone conference, to be provided at no cost to the individual. Also, unless otherwise agreed, the language used in the arbitration will be English; however, upon a reasoned request, interpretation at the arbitral hearing and translation will normally[19] be provided at no cost to the data subject, who moreover may be assisted by his or her national DPA in preparing his or her claim. While each party has to bear its own attorney's fees, if represented by an attorney before the panel, the Department of Commerce will establish a fund supplied with annual contributions by the Privacy Shield organisations, which shall cover the eligible costs of the arbitration procedure, up to maximum amounts, to be determined by the U.S. authorities in consultation with the Commission.

(47) The Privacy Shield Panel will have the authority to impose "individual-specific, non-monetary equitable relief"[20] necessary to remedy non-compliance with the Privacy

---

[17] See the Supplemental Principle on “The Role of the Data Protection Authorities” (Sec. III.5.c of the Privacy Principles set out in Annex II).

[18] The number of arbitrators on the panel will have to be agreed between the parties.

[19] However, the panel may find that, under the circumstances of the specific arbitration, coverage would lead to unjustified or disproportionate costs.

[20] Individuals may not claim damages in arbitration, but in turn invoking arbitration will not foreclose the option to seek damages in the ordinary U.S. courts.

Principles. While the panel will take into account other remedies already obtained by other Privacy Shield mechanisms when making its determination, individuals may still resort to arbitration if they consider these other remedies to be insufficient. This will allow EU data subjects to invoke arbitration in all cases where the action or inaction of the competent U.S. authorities (for instance the FTC) has not satisfactorily resolved their complaints. Arbitration may not be invoked if a DPA has the legal authority to resolve the claim at issue with respect to the U.S. self-certified company, namely in those cases where the organisation is either obliged to cooperate and comply with the advice of the DPAs as regards the processing of human resources data collected in the employment context, or has voluntarily committed to do so. Individuals can enforce the arbitration decision in the U.S. courts under the Federal Arbitration Act, thereby ensuring a legal remedy in case a company fails to comply.

(48) Where an organisation does not comply with its commitment to respect the Principles and published privacy policy, additional avenues for judicial redress may be available under the law of the U.S. States which provide for legal remedies under tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract.

(49) In the light of the information in this section, the Commission considers that the Privacy Principles issued by the U.S. Department of Commerce as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the substantive basic principles laid down in Directive 95/46/EC.

(50) In addition, the effective application of the Privacy Principles is guaranteed by the transparency obligations and the administration of the Privacy Shield by the Department of Commerce.

(51) Moreover, the Commission considers that, taken as a whole, the oversight and recourse mechanisms provided for by the Privacy Shield enable infringements of the Privacy Principles by Privacy Shield organisations to be identified and punished in practice and offer legal remedies to the data subject to gain access to personal data relating to him and, eventually, to obtain the rectification or erasure of such data.

3. Access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities

(52) As follows from Annex II, Sec. I.5, adherence to the Privacy Principles is limited to the extent necessary to meet national security, public interest or law enforcement requirements.

(53) The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence[21], has provided the Commission with detailed representations

[21] The Office of the Director of National Intelligence (ODNI) serves as the head of the Intelligence Community and acts as the principal advisor to the President and the National Security Council. See the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 of 17.12.2004. Among others, the ODNI shall determine requirements for, and manage and direct the tasking, collection, analysis, production and dissemination of national intelligence by the Intelligence Community, including by

and assurances that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community. Finally, a representation from the U.S. Department of Justice, contained in Annex VII to this decision, describes the limitations and safeguards applicable to access and use of data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.

(54) The findings of the Commission on the limitations on access and use of personal data transferred from the European Union to the United States by U.S. public authorities and the existence of effective legal protection are further elaborated below.

3.1. Access and use by U.S. public authorities for national security purposes

(55) The Commission’s analysis shows that U.S. law contains clear limitations on the access and use of personal data transferred under the EU-U.S. Privacy Shield for national security purposes as well as oversight and redress mechanisms that provide sufficient safeguards for those data to be effectively protected against unlawful interference and the risk of abuse.[22] Since 2013, when the Commission issued its two Communications (see recital (7)), this legal framework has been significantly strengthened.

3.1.1. Limitations

(56) Under the U.S. Constitution, ensuring national security falls within the President's authority as Commander in Chief, as Chief Executive and, as regards foreign intelligence, to conduct U.S. foreign affairs.[23] While Congress has the power to impose limitations, and has done so in various respects, within these boundaries the President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives. This of course also applies in those areas where no Congressional guidance exists. At present, the two central legal instruments in this regard are Executive Order 12333 ("E.O. 12333")[24] and Presidential Policy Directive 28.

(57) Presidential Policy Directive 28 ("PPD-28"), issued on 17 January 2014, imposes a number of limitations for "signals intelligence" operations.[25] This presidential directive has binding force for U.S. intelligence authorities[26] and remains effective

---

developing guidelines for how information or intelligence is accessed, used and shared. See Sec. 1.3 (a), (b) of E.O. 12333.

22 See *Schrems*, paragraph 91.

23 U.S. Const., Article II. See also the introduction to PPD-28.

24 E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981). To the extent that the Executive Order is publicly accessible, it defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities (in particular the need to promulgate specific procedural rules). According to Sec. 3.2 of E.O. 12333, the President, supported by the National Security Council, and the DNI shall issue such appropriate directives, procedures and guidance as are necessary to implement the order.

25 According to E.O. 12333, the Director of the National Security Agency (NSA) is the Functional Manager for signals intelligence and shall operate a unified organization for signals intelligence activities.

26 For the definition of the term "Intelligence Community", see Sec. 3.5 (h) of E.O. 12333 with n. 1 of PPD-28.

upon change in the U.S. Administration[27]. PPD-28 is of particular importance for non-US persons, including EU data subjects. Among others, it stipulates that:

(a) the collection of signals intelligence must be based on statute or Presidential authorisation, and must be undertaken in accordance with the U.S. Constitution (in particular the Fourth Amendment) and U.S. law;

(b) all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside;

(c) all persons have legitimate privacy interests in the handling of their personal information;

(d) privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities;

(e) U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of their nationality or where they might reside.

(58) PPD-28 directs that signals intelligence may be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purpose (e.g. to afford a competitive advantage to U.S. companies). Furthermore, it directs that collection shall always[28] be "as tailored as feasible", and that the Intelligence Community shall prioritise the availability of other information and appropriate and feasible alternatives.[29]

(59) In this regard, the representations of the Office of the Director of National Intelligence (ODNI) provide further assurance that these requirements, including the definition of bulk collection in PPD-28 (n. 5), express a general rule of prioritisation of targeted over bulk collection. According to these representations, Intelligence Community elements "should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (*e.g.* specific facilities, selection terms and identifiers)."[30] While PPD-28 explains that Intelligence Community elements must sometimes collect bulk signals intelligence in certain circumstances, for instance in order to identify new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence.[31] Hence, bulk collection will only be allowed where targeted collection via the use of discriminants is not possible "due to technical or operational considerations".[32] This applies both to the manner in which signals

[27] See Memorandum by the Office of Legal Counsel, Department of Justice, to President Clinton, 29.01.2000. According to this legal opinion, presidential directives have the "same substantive legal effect as an Executive Order".

[28] See ODNI Representations (Annex VI), p. 3.

[29] It should also be noted that, according to Sec. 2.4 of E.O. 12333, elements of the IC "shall use the least intrusive collection techniques feasible within the United States".

[30] ODNI Representations (Annex VI), p. 3.

[31] See also Sec. 5(d) of PPD-28 which directs the Director of National Intelligence, in coordination with the heads of relevant Intelligence Community elements and the Office of Science and Technology Policy, to provide the President with a "report assessing the feasibility of creating software that would allow the Intelligence Community more easily to conduct targeted information acquisition rather than bulk collection." According to public information, the result of this report was that "there is no software-based alternative which will provide a complete substitute for bulk collection in the detection of some national security threats." See Signals Intelligence Reform, 2015 Anniversary Report.

[32] See ODNI Representations (Annex VI), p. 3.

intelligence is collected and to what is actually collected.[33] According to representations of the ODNI all this ensures that the exception does not swallow the rule.[34]

(60) Furthermore, the representations of the ODNI provide assurance that decisions about what is "feasible" are not left to the discretion of individual intelligence agents, but are subject to the policies and procedures that the various U.S. Intelligence Community elements (agencies) are required to put in place to implement PPD-28.[35] Also, the research and determination of appropriate selectors takes place within the overall "National Intelligence Priorities Framework" (NIPF) which ensures that intelligence priorities are set by high-level policymakers and regularly reviewed to remain responsive to actual national security threats and taking into account possible risks, including privacy risks.[36] On this basis, agency personnel researches and identifies specific selection terms expected to collect foreign intelligence responsive to the priorities.[37] Selectors must be regularly reviewed to see if they still provide valuable intelligence in line with the priorities.[38]

(61) Finally, even where the United States considers it necessary to collect signals intelligence in bulk, under the conditions set out in recitals (58)-(60), PPD-28 limits the use of such information to a specific list of six national security purposes with a view to protect the privacy and civil liberties of all persons, whatever their nationality and place of residence.[39] These permissible purposes comprise measures to detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, to the Armed Forces or military personnel, as well as transnational criminal threats related to the other five purposes, and will be reviewed at least on an annual basis. According to the representations by the U.S. government, Intelligence Community elements have reinforced their analytic practices and standards for querying unevaluated signals intelligence to conform with these requirements; the use of targeted queries "ensures that only those items believed to be of potential intelligence value are ever presented to analysts to examine."[40]

(62) These limitations are particularly relevant to personal data transferred under the EU-U.S. Privacy Shield, in particular in case access to personal data were to take place outside the United States, including during their transit on the transatlantic cables from the Union to the United States. As confirmed by the U.S. authorities in the representations of the ODNI, the limitations and safeguards set out therein – including those of PPD-28 – apply to such access.[41]

---

33 ODNI Representations (Annex VI), p. 3.

34 ODNI Representations (Annex VI), p. 4.

35 See Sec. 4(b),(c) of PPD-28. According to public information, the 2015 review confirmed the existing six purposes. See ODNI, Signals Intelligence Reform, 2016 Progress Report.

36 ODNI Representations (Annex VI), p. 6 (with reference to Intelligence Community Directive 204). See also Sec. 3 of PPD-28.

37 ODNI Representations (Annex VI), p. 6. See, for instance, NSA Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014. See also ODNI Status Report 2014. For access requests under Sec. 702 FISA, queries are governed by the FISC-approved minimization procedures. See NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014.

38 See Signal Intelligence Reform, 2015 Anniversary Report. See also ODNI Representations (Annex VI), pp. 6, 8-9, 11.

39 See Sec. 2 of PPD-28.

40 ODNI Representations (Annex VI), p. 4. See also Intelligence Community Directive 203.

41 ODNI Representations (Annex VI), p. 2. Likewise, the limitations stipulated in E.O. 12333 (e.g. the need for collected information to respond to intelligence priorities set by the President) apply.

(63) Although not phrased in those legal terms, these principles capture the essence of the principles of necessity and proportionality. Targeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical or operational reasons. Even where *bulk collection* cannot be avoided, further "use" of such data through access is *strictly limited* to specific, legitimate national security purposes.[42]

(64) As a directive issued by the President as the Chief Executive, these requirements bind the entire Intelligence Community and have been further implemented through agency rules and procedures that transpose the general principles into specific directions for day-to-day operations. Moreover, while Congress is itself not bound by PPD-28, it has also taken steps to ensure that collection and access of personal data in the United States are targeted rather than carried out "on a generalised basis".

(65) It follows from the available information, including the representations received from the U.S. government, that once the data has been transferred to organisations located in the United States and self-certified under the EU-U.S. Privacy Shield, U.S. intelligence agencies may only[43] seek personal data where their request complies with the Foreign Intelligence Surveillance Act (FISA) or is made by the Federal Bureau of Investigation based on a so-called National Security Letter (NSL)[44]. Several legal bases exist under FISA that may be used to collect (and subsequently process) the personal data of EU data subjects transferred under the EU-U.S. Privacy Shield. Aside from traditional individualised electronic surveillance under Section 104 FISA[45] and the installation of pen registers or trap and trace devices under Section 402 FISA[46], the two central instruments are Section 501 FISA (ex-Section 215 U.S. PATRIOT ACT) and Section 702 FISA.[47]

---

[42] See *Schrems*, paragraph 93.

[43] In addition, the collection of data by the FBI may also be based on law enforcement authorizations (see Section 3.2 of this decision).

[44] For further explanations on the use of NSL see ODNI Representations (Annex VI), pp. 13-14 with n. 38. As indicated therein, the FBI may resort to NSLs only to request non-content information relevant to an authorized national security investigation to protect against international terrorism or clandestine intelligence activities. As regards data transfers under the EU-U.S. Privacy Shield, the most relevant legal authorization appears to be the Electronic Communications Privacy Act (18 U.S.C. § 2709), which requires that any request for subscriber information or transactional records uses a "term that specifically identifies a person, entity, telephone number, or account".

[45] 50 U.S.C. § 1804. While this legal authority requires a "statement of the facts and circumstances relied upon by the applicant to justify his belief that (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power", the latter may include non-U.S. persons that engage in international terrorism or the international proliferation of weapons of mass destruction (including preparatory acts) (50 U.S.C. § 1801 (b)(1)). Still, there is only a theoretical link to personal data transferred under the EU-U.S. Privacy Shield, given that the statement of facts also has to justify the belief that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power". In any event, the use of this authority requires application to the FISC which will assess, among others, whether on the basis of the submitted facts there is probable cause that this is indeed the case.

[46] 50 U.S.C. § 1842 with § 1841(2) and Sec. 3127 of Title 18. This authority does not concern the contents of communications, but rather aims at information about the customer or subscriber using a service (such as name, address, subscriber number, length/type of service received, source/mechanism of payment). It requires an application for an order by the FISC (or a U.S. Magistrate Judge) and the use of a specific selection term in the sense of § 1841(4), i.e. a term that specifically identifies a person, account, etc. and is used to limit, to the greatest extent reasonably possible, the scope of the information sought.

[47] While Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT) authorizes the FBI to request a court order aiming at the production of "tangible things" (in particular telephone metadata, but also business records) for foreign intelligence purposes, Sec. 702 FISA allows US Intelligence Community elements to seek access to

(66) In this respect, the USA FREEDOM Act, which was adopted on 2 June 2015, prohibits the collection in bulk of records based on Section 402 FISA (pen register and trap and trace authority), Section 501 FISA (formerly: Section 215 of the U.S. PATRIOT ACT)[48] and through the use of NSL, and instead requires the use of specific "selection terms".[49]

(67) While the FISA contains further legal authorisations to carry out national intelligence activities, including signals intelligence, the Commission's assessment has shown that, insofar as personal data to be transferred under the EU-U.S. Privacy Shield are concerned, these authorities equally restrict public interference to targeted collection and access.

(68) This is clear for traditional individualised electronic surveillance under Section 104 FISA[50]. As for Section 702 FISA, which provides the basis for two important intelligence programs run by the U.S. intelligence agencies (PRISM, UPSTREAM), searches are carried out in a targeted manner through the use of individual selectors that identify specific communications facilities, like the target's email address or telephone number, but not key words or even the names of targeted individuals.[51] Therefore, as noted by the Privacy and Civil Liberties Oversight Board (PCLOB), Section 702 surveillance "consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made".[52] Due to a "sunset" clause, Section 702 FISA will have to be reviewed in 2017, at which time the Commission will have to reassess the safeguards available to EU data subjects.

(69) Moreover, in its representations the U.S. government has given the European Commission explicit assurance that the U.S. Intelligence Community "does not engage in indiscriminate surveillance of anyone, including ordinary European citizens"[53]. As regards personal data collected within the United States, this statement is supported by empirical evidence which shows that *access requests* through NSL and under FISA,

---

information, including the content of internet communications, from within the United States, but targeting certain non-U.S. persons outside the United States.

48 Based on this provision, the FBI may request "tangible things" (e.g. records, papers, documents) based on a showing to the Foreign Intelligence Surveillance Court (FISC) that there are reasonable grounds to believe that they are relevant to a specific FBI investigation. In carrying out its search, the FBI must use FISC-approved selection terms for which there is a "reasonable, articulable suspicion" that such term is associated with one or more foreign powers or their agents engaged in international terrorism or activities in preparation therefore. See PCLOB, Sec. 215 Report, p. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016, pp. 4-6.

49 ODNI Representations (Annex VI), p. 13 (n. 38).

50 See footnote 45.

51 PCLOB, Sec. 702 Report, pp. 32-33 with further references. According to its privacy office, the NSA must verify that there is a connection between the target and the selector, must document the foreign intelligence information expected to be acquired, this information must be reviewed and approved by two senior NSA analysts, and the overall process will be tracked for subsequent compliance reviews by the ODNI and Department of Justice. See NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.04.2014.

52 PLCOB, Sec. 702 Report, p. 111. See also ODNI Representations (Annex VI), p. 9 ("Collection under Section 702 of the [FISA] is not 'mass and indiscriminate' but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets") and p. 13, n. 36 (with reference to a 2014 FISC Opinion); NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.04.2014. Even in the case of UPSTREAM, the NSA may only request the interception of electronic communications to, from, or about tasked selectors.

53 ODNI Representations (Annex VI), p. 18. See also p. 6, according to which the applicable procedures "demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information, and to implement – from the highest levels of our Government – the principle of reasonableness."

both individually and together, only concern a relatively small number of targets when compared to the overall flow of data on the internet.[54] Moreover, the U.S. government has assured the Commission that "any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet."[55] This statement also covers possible access to the transatlantic cables (which the U.S. government neither confirms nor denies is taking place).

(70) As regards *access* to collected data and *data security*, PPD-28 requires that access "shall be limited to authorized personnel with a need to know the information to perform their mission" and that personal information "shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information". Intelligence personnel receive appropriate and adequate training in the principles set forth in PPD-28.[56]

(71) Finally, as regards the *storage* and further *dissemination* of personal data from EU data subjects collected by U.S. intelligence authorities, PPD-28 states that all persons (including non-U.S. persons) should be treated with dignity and respect, that all persons have legitimate privacy interests in the handling of their personal data and that Intelligence Community elements therefore have to establish policies providing appropriate safeguards for such data "reasonably designed to minimize the[ir] dissemination and retention".

(72) The U.S. government has explained that this reasonableness requirement signifies that Intelligence Community elements will not have to adopt "any measure theoretically possible", but will need to "balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities."[57] In this respect, non-U.S. persons will be treated in the same way as U.S. persons, based on procedures approved by the Attorney-General.[58]

(73) According to these rules, retention is generally limited to a maximum of five years, unless there is a specific determination in law or an express determination by the

---

54 See Statistical Transparency Report Regarding Use of National Security Authorities, 22.04.2015. For the overall flow of data on the internet, see for example Fundamental Rights Agency, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), at pp. 15-16. As regards the UPSTREAM program, according to a declassified FISC opinion of 2011, over 90% of the electronic communications acquired under Sec. 702 FISA came from the PRISM program, whereas less than 10% came from UPSTREAM. See FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (available at: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

55 ODNI Representations (Annex VI), p. 4.

56 See Sec. 4(a)(ii) of PPD-28. See also ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, July 2014, p. 5, according to which "Intelligence Community element policies should reinforce existing analytic practices and standards whereby analysts must seek to structure queries or other search terms and techniques to identify intelligence information relevant to a valid intelligence or law enforcement task; focus queries about persons on the categories of intelligence information responsive to an intelligence or law enforcement requirement; and minimize the review of personal information not pertinent to intelligence or law enforcement requirements." See e.g. CIA, Signals Intelligence Activities, p. 5; FBI, Presidential Policy Directive 28 Policies and Procedures, p. 3. According to the 2016 Progress Report on the Signals Intelligence Reform, IC elements (including the FBI, CIA and NSA) have taken steps to sensitise their personnel to the requirements of PPD-28 by creating new or modifying existing training policies.

57 ODNI Representations (Annex VI), p. 4.

58 See Sec. 4(a)(i) of PPD-28 with Sec 2.3 of E.O. 12333.

Director of National Intelligence after careful evaluation of privacy concerns – taking into account the views of the ODNI Civil Liberties Protection Officer as well as agency privacy and civil liberties officials – that continued retention is in the interest of national security.[59] Dissemination is limited to cases where the information is relevant to the underlying purpose of the collection and thus responsive to an authorised foreign intelligence or law enforcement requirement.[60]

(74) According to the assurances given by the U.S. government, personal information may not be disseminated solely because the individual concerned is a non-U.S. person and "signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement."[61]

(75) The Commission therefore concludes that there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question.

3.1.2. Effective legal protection

(76) The Commission has assessed both the oversight mechanisms that exist in the United States with regard to any interference by U.S. intelligence authorities with personal data transferred to the United States and the avenues available for EU data subjects to seek individual redress.

Oversight

(77) First, intelligence activities by U.S. authorities are subject to extensive oversight from within the executive branch.

(78) According to PPD-28, Section 4(a)(iv), the policies and procedures of Intelligence Community elements "shall include appropriate measures to facilitate oversight over

---

59 Sec. 4(a)(i) of PPD-28; ODNI Representations (Annex VI), p. 7. For instance, for personal information collected under Sec. 702 FISA, the NSA's FISC-approved minimization procedures foresee as a rule that the metadata and unevaluated content for PRISM is retained for no more than five years, whereas UPSTREAM data is retained for no more than two years. The NSA complies with these storage limits through an automated process that deletes collected data at the end of the respective retention period. See NSA Sec. 702 FISA Minimization Procedures, Sec. 7 with Sec. 6(a)(1); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014. Likewise, retention under Sec. 501 FISA (ex-Sec. 2015 U.S. PATRIOT ACT) is limited to five years, unless the personal data form part of properly approved dissemination of foreign intelligence information, or if the DOJ advises the NSA in writing that the records are subject to a preservation obligation in pending or anticipated litigation. See NSA, CLOP, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016.

60 In particular, in case of Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT), dissemination of personal information may take place only for counterterrorism purposes or as evidence of a crime; in case of Sec. 702 FISA only if there is a valid foreign intelligence or law enforcement purpose. Cf. NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016. See also NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014.

61 ODNI Representations (Annex VI), p. 7 (with reference to Intelligence Community Directive (ICD) 203).

the implementation of safeguards protecting personal information"; these measures should include periodic auditing.[62]

(79) Multiple oversight layers have been put in place in this respect, including civil liberties or privacy officers, Inspector Generals, the ODNI Civil Liberties and Privacy Office, the PCLOB, and the President's Intelligence Oversight Board. These oversight functions are supported by compliance staff in all the agencies.[63]

(80) As explained by the U.S. government[64], *civil liberties or privacy officers* with oversight responsibilities exist at various departments with intelligence responsibilities and intelligence agencies.[65] While the specific powers of these officers may vary somewhat depending on the authorising statute, they typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated (and in some cases, like the ODNI, may themselves have the power to investigate complaints[66]). The head of the department/agency in turn has to ensure that the officer receives all the information and is given access to all material necessary to carry out his functions. Civil liberties and privacy officers periodically report to Congress and the PCLOB, including on the number and nature of the complaints received by the department/agency and a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the officer.[67]

(81) In addition, each Intelligence Community element has its own *Inspector General* with responsibility, among others, to oversee foreign intelligence activities.[68] This includes, within the ODNI, an Office of the Inspector General with comprehensive jurisdiction over the entire Intelligence Community and authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority, in connection with ODNI and/or Intelligence Community programs and activities.[69] Inspectors General are statutorily independent[70] units responsible for conducting

[62] ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, p. 7. See e.g. CIA, Signals Intelligence Activities, p. 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 8.1, 8.6(c).

[63] For instance, the NSA employs more than 300 compliance staff in the Directorate for Compliance. See ODNI Representations (Annex VI), p. 7.

[64] See Ombudsperson Mechanism (Annex III), Sec. 6(b) (i) to (iii).

[65] See 42 U.S.C. § 2000ee-1. This includes for instance the Department of State, the Department of Justice (including the FBI), the Department of Homeland Security, the Department of Defense, the NSA, CIA and the ODNI.

[66] According to the U.S. government, if the ODNI Civil Liberties and Privacy Office receives a complaint, it will also coordinate with other Intelligence Community elements on how that complaint should be further processed within the IC. See Ombudsperson Mechanism (Annex III), Sec. 6(b) (ii).

[67] See 42 U.S.C. § 2000ee-1 (f)(1),(2).

[68] ODNI Representations (Annex VI), p. 7. See e.g. NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 8.1; CIA, Signals Intelligence Activities, p. 7 (Responsibilities).

[69] This IG (which was created in October 2010) is appointed by the President, with Senate confirmation, and can be removed only by the President, not the DNI.

[70] These IGs have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal. This does not necessarily mean that they are completely free from instructions. In some cases, the head of the department may prohibit the Inspector General from initiating, carrying out, or completing an audit or investigation where this is considered necessary to preserve important national (security) interests. However, Congress must be informed of the exercise of this authority and on this basis could hold the respective director responsible. See, e.g., Inspector

audits and investigations relating to the programs and operations carried out by the respective agency for national intelligence purposes, including for abuse or violation of the law.[71] They are authorised to have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony.[72] While the Inspectors General can only issue non-binding recommendations for corrective action, their reports, including on follow-up action (or the lack thereof) are made public and moreover sent to Congress which can on this basis exercise its oversight function.[73]

(82) Furthermore, the *Privacy and Civil Liberties Oversight Board*, an independent agency within the executive branch composed of members[74] appointed by the President with Senate approval, is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. For these purposes, it may access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony. It receives reports from the civil liberties and privacy officers of several federal departments/agencies[75], may issue recommendations to them, and regularly reports to Congressional committees and the President.[76] The PCLOB is also tasked, within the confines of its mandate, to prepare a report assessing the implementation of PPD-28.

(83) Finally, the aforementioned oversight mechanisms are complemented by the *Intelligence Oversight Board* established within the President's Intelligence Advisory Board which oversees compliance by US intelligence authorities with the Constitution and all applicable rules.

(84) To facilitate the oversight, Intelligence Community elements are encouraged to design information systems to allow for the monitoring, recording and reviewing of queries or other searches of personal information.[77] Oversight and compliance bodies will periodically check the practices of Intelligence Community elements for protecting personal information contained in signals intelligence and their compliance with those procedures.[78]

(85) These oversight functions are moreover supported by extensive reporting requirements with respect to non-compliance. In particular, agency procedures must ensure that, when a significant compliance issue occurs involving personal information of any

---

General Act of 1978, § 8 (IG of the Department of Defense); § 8E (IG of the DOJ), § 8G (d)(2)(A),(B) (IG of the NSA); 50. U.S.C. § 403q (b) (IG for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (IG for the Intelligence Community).

71 See ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, as amended, Pub. L. 113-126 of 7.07.2014.

72 See Inspector General Act of 1978, § 6.

73 See ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, §§ 4(5), 5. According to Sec. 405(b)(3),(4) of the Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 of 7.10.2010, the IG for the Intelligence Community will keep the DNI as well as Congress informed of the necessity for, and the progress of, corrective actions.

74 In addition, the PCLOB employs some 20 regular staff. See https://www.pclob.gov/about-us/staff.html.

75 These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, the Director of National Intelligence and the Central Intelligence Agency, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

76 See 42 U.S.C. § 2000ee. See also Ombudsperson Mechanism (Annex III), Sec. 6(b) (iv).

77 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, pp. 7-8.

78 Id. at p. 8. See also ODNI Representations (Annex VI), p. 9.

person, regardless of nationality, collected through signals intelligence, such issue shall be promptly reported to the head of the Intelligence Community element, which in turn will notify the Director of National Intelligence who, under PPD-28, shall determine if any corrective actions are necessary.[79] Moreover, according to E.O. 12333, all Intelligence Community elements are required to report to the Intelligence Oversight Board on non-compliance incidents.[80] These mechanisms ensure that the issue will be addressed at the highest level in the Intelligence Community. Where it involves a non-U.S. person, the Director of National Intelligence, in consultation with the Secretary of State and the head of the notifying department or agency, shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.[81]

(86) Second, in addition to these oversight mechanisms within the executive branch, the U.S. Congress, specifically the *House and Senate Intelligence and Judiciary Committees*, have oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence. According to the National Security Act, "[t]he President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter."[82] Also, "[t]he President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity."[83] Members of these committees have access to classified information as well as intelligence methods and programs.[84]

(87) Later statutes have extended and refined the reporting requirements, both regarding the Intelligence Community elements, the relevant Inspector Generals and the Attorney-General. For instance, FISA requires the Attorney General to "fully inform" the Senate and House Intelligence and Judiciary Committees regarding the government's activities under certain sections of FISA.[85] It also requires the government to provide the Congressional committees with copies of "all decisions, orders, or opinions of the FISC or that include significant construction or interpretation" of FISA provisions. In particular, as regards surveillance under Section 702 FISA, oversight is exercised through statutorily required reports to the Intelligence and Judiciary Committees, as well as frequent briefings and hearings. These include a semi-annual report by the Attorney General describing the use of Section 702 FISA, with supporting documents including notably the Department of Justice and ODNI compliance reports and a description of any incidents of non-compliance,[86] and a separate semi-annual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures

79 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, p. 7. See, e.g., NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 7.3, 8.7(c),(d); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III.(A)(4), (B)(4); CIA, Signals Intelligence Activities, p. 6 (Compliance) and p. 8 (Responsibilities).

80 See E.O. 12333, Sec. 1.6(c).

81 PPD-28, Sec. 4(a)(iv).

82 See Sec. 501(a)(1) (50 U.S.C. § 413(a)(1)). This provision contains the general requirements as regards Congressional oversight in the area of national security.

83 See Sec. 501(b) (50 U.S.C. § 413(b)).

84 Cf. Sec. 501(d) (50 U.S.C. § 413(d)).

85 See 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

86 See 50 U.S.C. § 1881f.

designed to ensure that collection is for a valid foreign intelligence purpose.[87] Congress also receives reports by the Inspector Generals who are authorised to evaluate the agencies' compliance with targeting and minimization procedures and Attorney General Guidelines.

(88) According to the USA FREEDOM Act of 2015, the U.S. government must disclose to Congress (and the public) each year the number of FISA orders and directives sought and received, as well as estimates of the number of U.S. and non-U.S. persons targeted by surveillance, among others.[88] The Act also requires additional public reporting about the number of NSL issued, again both with regard to U.S. and non-U.S. persons (while at the same time allowing the recipients of FISA orders and certifications, as well as NSL requests, to issue transparency reports under certain conditions).[89]

(89) Third, intelligence activities by U.S. public authorities based on FISA allow for review, and in some cases prior authorisation of the measures, by the *FISA Court* (FISC)[90], an independent tribunal[91] whose decisions can be challenged before the Foreign Intelligence Court of Review (FISCR)[92] and, ultimately, the Supreme Court of the United States.[93] In case of prior authorisation, the requesting authorities (FBI, NSA, CIA, etc.) will have to submit a draft application to lawyers at the National Security Department of the Department of Justice who will scrutinise it and, if necessary, request additional information.[94] Once the application has been finalised, it will have to be approved by the Attorney General, Deputy Attorney General or the Assistant Attorney General for National Security.[95] The Department of Justice will then submit the application to the FISC that will assess the application and make a

---

87 See 50 U.S.C. § 1881a(l)(1).

88 See USA FREEDOM Act of 2015, Pub. L. No. 114-23, Sec. 602(a). In addition, according to Sec 402, "the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion."

89 USA FREEDOM Act, Sec. 602(a), 603(a).

90 For certain types of surveillance, alternatively a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States may have the power to hear applications and grant orders.

91 The FISC is comprised of eleven judges appointed by the Chief Justice of the United States from among sitting U.S. district court judges, who previously have been appointed by the President and confirmed by the Senate. The judges have life tenure, can only be removed for good cause and serve on the FISC for staggered seven-year terms. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits. See Sec 103 FISA (50 U.S.C. 1803 (a)); PCLOB, Sec. 215 Report, pp. 174-187. The judges are supported by experienced judicial law clerks that constitute the court's legal staff and prepare legal analysis on collection requests. See PCLOB, Sec. 215 Report, p. 178; Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (July 29, 2013) ("Walton Letter"), pp. 2-3.

92 The FISCR is composed of three judges appointed by the Chief Justice of the United States and drawn from U.S. district courts or courts of appeals, serving for a staggered seven year term. See Sec. 103 FISA (50 U.S.C. § 1803 (b)).

93 See 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

94 For instance, additional factual details about the target of the surveillance, technical information about the surveillance methodology, or assurances about how the information acquired will be used and disseminated. See PCLOB, Sec. 215 Report, p. 177.

95 50 U.S.C. §§ 1804 (a), 1801 (g).

preliminary determination on how to proceed.[96] Where a hearing takes place, the FISC has the authority to take testimony which may include expert advice.[97]

(90) The FISC (and FISCR) are supported by a standing panel of five individuals that have an expertise in national security matters as well as civil liberties.[98] From this group the court shall appoint an individual to serve as *amicus curiae* to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate.[99] This shall in particular ensure that privacy considerations are properly reflected in the court's assessment. The court may also appoint an individual or organisation to serve as *amicus curiae*, including providing technical expertise, whenever it deems this appropriate or, upon motion, permit an individual or organisation leave to file an *amicus curiae* brief.[100]

(91) As regards the two legal authorisations for surveillance under FISA that are most important for data transfers under the EU-U.S. Privacy Shield, oversight by the FISC differs.

(92) Under Section 501 FISA[101], which allows the collection of "any tangible things (including books, records, papers, documents, and other items)", the application to the FISC must contain a statement of facts showing that there are reasonable grounds to believe that the tangible things sought for are relevant to an authorised investigation (other than a threat assessment) conducted to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Also, the application must contain an enumeration of the minimisation procedures adopted by the Attorney General for the retention and dissemination of the collected intelligence. [102]

(93) Conversely, under Section 702 FISA[103], the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence. Section 702 FISA allows the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[104] Such targeting is carried out by the NSA in two steps: First, NSA analysts will identify non-U.S. persons located abroad whose surveillance will lead, based on the analysts' assessment, to the relevant foreign intelligence

---

96 The FISC may approve the application, request further information, determine the necessity of a hearing or indicate a possible denial of the application. On the basis of this preliminary determination, the government will make its final application. The latter may include substantial changes to the original application on the basis of the judge's preliminary comments. Although a large percentage of final applications are approved by the FISC, a substantial part of these contain substantive changes to the original application, e.g. 24% of applications approved for the period from July to September 2013. See PCLOB, Sec. 215 Report, p.179; Walton Letter, p. 3.

97 PCLOB, Sec. 215 Report, p.179, n. 619.

98 50 U.S.C. § 1803 (i)(1),(3)(A). This new legislation implemented recommendations by the PCLOB to establish a pool of privacy and civil liberties experts that can serve as *amicus curiae*, in order to provide the court with legal arguments to the advancement of privacy and civil liberties. See PCLOB, Sec. 215 Report, pp. 183-187.

99 50 U.S.C. § 1803 (i)(2)(A). According to information by the ODNI, such appointments have already taken place. See Signals Intelligence Reform, 2016 Progress Report.

100 50 U.S.C. § 1803 (i)(2)(B).

101 50 U.S.C. § 1861

102 50 U.S.C. § 1861 (b).

103 50 U.S.C. § 1881.

104 50 U.S.C. § 1881a (a).

specified in the certification. Second, once these individualised persons have been identified and their targeting has been approved by an extensive review mechanism within the NSA[105], selectors identifying communication facilities (such as email addresses) used by the targets will be "tasked".[106] As indicated, the certifications to be approved by the FISC contain no information about the individual persons to be targeted but rather identify categories of foreign intelligence information.[107] While the FISC does not assess – under a probable cause or any other standard – that individuals are properly targeted to acquire foreign intelligence information,[108] its control extends to the condition that "a significant purpose of the acquisition is to obtain foreign intelligence information"[109]. Indeed, under Section 702 FISA, the NSA is allowed to collect communications of non-U.S. persons outside the U.S. only if it can be reasonably believed that a given means of communication is being used to communicate foreign intelligence information (e.g. related to international terrorism, nuclear proliferation or hostile cyber activities). Determinations to this effect are subject to judicial review.[110] Certifications also need to provide for targeting and minimization procedures.[111] The Attorney General and the Director of National Intelligence verify compliance and the agencies have the obligation to report any incidents of non-compliance to the FISC[112] (as well as the Congress and the President's Intelligence Oversight Board), which on this basis can modify the authorisation.[113]

(94) Furthermore, to increase the efficiency of the oversight by the FISC, the U.S. Administration has agreed to implement a recommendation by the PCLOB to supply to the FISC documentation of Section 702 targeting decisions, including a random sample of tasking sheets, so as to allow the FISC to assess how the foreign intelligence purpose requirement is being met in practice.[114] At the same time, the U.S.

---

105 PCLOB, Sec. 702 Report, p. 46.

106 50 U.S.C. § 1881a (h).

107 50 U.S.C. § 1881a (g). According to the PCLOB, these categories have so far mainly concerned international terrorism and topics such as the acquisition of weapons of mass destruction. See PCLOB, Sec. 702 Report, p. 25.

108 PCLOB, Sec. 702 Report, p. 27.

109 50 U.S.C. § 1881a.

110 "Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12.12.2013, p. 152.

111 50 U.S.C.1881a (i).

112 Rule 13(b) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented in a manner that does not comply with the Court's authorization or approval, or with applicable law. It also requires the government to notify the Court in writing of the facts and circumstances relevant to such non-compliance. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. See Walton Letter, p. 10.

113 50 U.S.C. § 1881 (l). See also PCLOB, Sec. 702 Report, pp. 66-76; NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014. The collection of personal data for intelligence purposes under Sec 702 FISA is subject to both internal and external oversight within the executive branch. Among others, the internal oversight includes internal compliance programs to evaluate and oversee compliance with targeting and minimization procedures; reporting of non-compliance incidents, both internally and externally to the ODNI, Department of Justice, Congress and the FISC; and annual reviews sent to the same bodies. As for external oversight, it mainly consists in targeting and minimization reviews conducted by the ODNI, DOJ and Inspectors General, which in turn report to Congress and the FISC, including on non-compliance incidents. Significant compliance incidents must be reported to the FISC immediately, others in a quarterly report. See PCLOB, Sec. 702 Report, pp. 66-77.

114 PCLOB, Recommendations Assessment Report, 29.01.2015, p. 20.

Administration accepted and has taken measures to revise NSA targeting procedures to better document the foreign intelligence reasons for targeting decisions.[115]

Individual redress

(95) A number of avenues are available under U.S. law to EU data subjects if they have concerns whether their personal data have been processed (collected, accessed, etc.) by U.S. Intelligence Community elements, and if so, whether the limitations applicable in U.S. law have been complied with. These relate essentially to three areas: interference under FISA; unlawful, intentional access to personal data by government officials; and access to information under Freedom of Information Act (FOIA).[116]

(96) First, the Foreign Intelligence Surveillance Act provides a number of remedies, available also to non-U.S. persons, to challenge unlawful electronic surveillance. This includes the possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed (18 U.S.C. § 2712); to sue U.S. government officials in their personal capacity ("under colour of law") for money damages (50 U.S.C. § 1810); and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States (50 U.S.C. § 1806).[117]

(97) Second, the U.S. government referred the Commission to a number of additional avenues that EU data subjects could use to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes (i.e. the Computer Fraud Abuse Act, 18 U.S.C. § 1030; Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712; and Right to Financial Privacy Act, 12 U.S.C. § 3417). All of these causes of action concern specific data, targets and/or types of access (e.g. remote access of a Computer via the Internet) and are available under certain conditions (e.g. intentional/wilful conduct, conduct outside of official capacity, harm suffered).[118]

(98) Finally, the U.S. government has pointed to the FOIA as a means for non-U.S. persons to seek access to existing federal agency records, including where these contain the individual's personal data (5 U.S.C. § 552).[119] Given its focus, the FOIA does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. Even in this respect the possibilities appear to be limited as agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations.[120] This being

---

[115] PCLOB, Recommendations Assessment Report, 29.01.2015, p.16.

[116] In addition, Sec. 10 of the Classified Information Procedures Act provides that, in any prosecution in which the United States must establish that material constitutes classified information (e.g. because it requires protection against unauthorized disclosure for reasons of national security), the United States shall notify the defendant of the portions of the material that it reasonably expects to rely upon to establish the classified information element of the offense.

[117] ODNI Representations (Annex VI), p. 16.

[118] ODNI Representations (Annex VI), p. 17.

[119] Similar laws exist at State level.

[120] If this is the case, the individual will normally only receive a standard reply by which the agency declines either to confirm or deny the existence of any records. See *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

said, the use of such exceptions by national intelligence agencies can be challenged by individuals who can seek both administrative and judicial review.

(99) While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available courses of action are limited[121] and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing"[122], which restricts access to ordinary courts.[123]

(100) In order to provide for an additional avenue accessible for all EU data subjects, the U.S. government has decided to create a new mechanism, the Privacy Shield Ombudsperson, as set out in the letter from the U.S. Secretary of State to the Commission which is contained in Annex III to this decision. This mechanism builds on the designation, under PPD-28, of a Senior Coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond. In particular, according to the binding commitments from the U.S. government, the Privacy Shield Ombudsperson will guarantee that individual complaints are investigated and individuals receive independent confirmation that U.S. laws have been complied with or, in case of a violation of such laws, the non-compliance has been remedied.

(101) This mechanism contributes to ensuring individual redress and independent oversight.

(102) First, differently from a pure government-to-government mechanism, the Privacy Shield Ombudsperson will receive and respond to individual complaints. Such complaints can be addressed to the Member States bodies competent for the oversight of national security services and, eventually, a centralised EU individual complaint handling body that will channel them to the Privacy Shield Ombudsperson.[124] This will in fact benefit EU data subjects who can turn to a national (as well as a European) body 'close to home' and in their own language. It will be the task of such body to support the individual in making a request to the Privacy Shield Ombudsperson that contains the basic information and thus can be considered "complete". Importantly, the

---

[121] See ODNI Representations (Annex VI), p. 16. According to the explanations provided, the available courses of action either require the existence of *damage* (18 U.S.C. § 2712; 50 U.S.C. § 1810) or a showing that the *government intends to use or disclose information* obtained or derived from electronic surveillance of the person concerned against that person *in judicial or administrative proceedings* in the United States (50 U.S.C. § 1806). However, as the Court of Justice has repeatedly stressed, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the person concerned has suffered any adverse consequences on account of that interference. See *Schrems*, paragraph 89 with further references.

[122] This admissibility criterion stems from the 'case or controversy' requirement of the U.S. Const., Art. III.

[123] See *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). As regards the use of NSLs, the USA FREEDOM Act (Sec. 502(f)-503) provides that non-disclosure requirements must be periodically reviewed, and that *recipients* of NSL be notified when the facts no longer support a non-disclosure requirement (see ODNI Representations (Annex VI), p. 13). However, this does not ensure that the *EU data subject* would be informed that (s)he has been the target of an investigation.

[124] According to the Ombudsperson Mechanism (Annex III), Sec. 4(f), the Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of the "underlying processes" that may provide the requested relief (e.g. a FOIA access request, see Sec. 5), those communications will take place in accordance with the applicable procedures.

individual does not have to demonstrate that his/her personal data has in fact been accessed by the U.S. government through signals intelligence activities.

(103) Second, in carrying out her functions, the Privacy Shield Ombudsperson will be able to rely on the independent oversight and compliance review mechanisms existing in U.S. law that involve bodies with the power to investigate the respective request and address non-compliance, such as the Inspector Generals and Civil Liberties and Privacy Officers.[125] Also, the Privacy Shield Ombudsperson will be able to refer matters to the PCLOB for its consideration.[126]

(104) Finally, the Privacy Shield Ombudsperson will be independent and thus free from instructions by the U.S. Intelligence Community. This is of significant importance, given that the Ombudsperson will have to "confirm" that the complaint has been properly investigated and that U.S. law – including the limitations and safeguards set out in the representations by the ODNI – has been complied with or, in the event of non-compliance, such violation has been remedied.[127] In order to be able to provide that independent confirmation, the Privacy Shield Ombudsperson will have to receive sufficient information to make an own assessment, both as regards the investigation carried out and the compliance of the respective national intelligence activities with U.S. law.

(105) The Commission therefore concludes that the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield.

3.2. Access and use by U.S. public authorities for law enforcement and public interest purposes

(106) As regards interference with personal data transferred under the EU-U.S. Privacy Shield for law enforcement purposes, the U.S. government (through the Department of Justice) has provided assurance on the applicable limitations and safeguards which in the Commission's assessment demonstrate an adequate level of protection.

(107) According to this information, under the Fourth Amendment of the U.S. Constitution searches and seizures by law enforcement authorities principally require a court-ordered warrant upon a showing of "probable cause". In the few specifically established and exceptional cases where the warrant requirement does not apply[128],

[125] See Ombudsperson Mechanism (Annex III), Sec. 2(a). See also recitals (80)-(81).

[126] See Ombudsperson Mechanism (Annex III), Sec. 2(c). According to the explanations provided by the U.S. government, the PCLOB shall continually review the policies and procedures, as well as their implementation, of those U.S. authorities responsible for counterterrorism to determine whether their actions "appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties." It also shall "receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities."

[127] Given that the Privacy Shield Ombudsperson "will neither confirm nor deny whether the individual has been the target of surveillance" (nor the specific remedy that was applied), the Commission considers that the caveat that any response will be "subject to the continuing obligation to protect information under applicable laws and policies" will not undermine the obligation to provide an appropriate response. The Commission will monitor, including through the Annual Joint Review, that this is indeed the case.

[128] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

law enforcement is subject to a "reasonableness" test.[129] Whether a search or seizure is reasonable is "determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[130] More generally, the Fourth Amendment guarantees privacy, dignity, and protects against arbitrary and invasive acts by officers of the Government.[131] These concepts capture the idea of necessity and proportionality in Union law.

(108) While the protection under the Fourth Amendment does not extend to non-U.S. persons that are not resident in the United State, the latter nevertheless benefit indirectly through the protection afforded to the U.S. companies holding the personal data and who are the recipients of law enforcement requests. Further protections are provided by special statutory authorities, as well as the Department of Justice Guidelines which limit law enforcement access to data on grounds equivalent to necessity and proportionality (e.g. by requiring that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties).[132] According to the representations made by the U.S. government, the same or higher protections apply to law enforcement investigations at State level (with respect to investigations carried out under State laws).[133]

(109) Although a prior judicial authorisation by a court or grand jury (an investigate arm of the court impanelled by a judge or magistrate) is not required in all cases[134], administrative subpoenas are limited to specific cases and will be subject to independent judicial review at least where the government seeks enforcement in court.[135]

(110) The same applies for the use of administrative subpoenas for public interest purposes. In addition, according to the representations from the U.S. government, similar substantive limitations apply in that agencies may only seek access to data that is relevant to matters falling with their scope of authority and have to respect the standard of reasonableness.

(111) The Commission therefore concludes that there are rules in place in the United States designed to limit any interference for law enforcement or other public interest purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question, and that ensure effective legal protection against such interference.

---

[129] PCLOB, Sec. 215 Report, p. 107, referring to *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

[130] PCLOB, Sec. 215 Report, p.107, referring to *Samson v. California*, 547 U.S. 843, 848 (2006).

[131] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

[132] DOJ Representations (Annex VII), p. 4 with further references.

[133] DOJ Representations (Annex VII), n. 2.

[134] According to the information the Commission has received, and leaving aside specific areas likely not relevant for data transfers under the EU-U.S. Privacy Shield (e.g. investigations into health care fraud, child abuse or controlled substances cases), this concerns mainly certain authorities under the Electronic Communications Privacy Act (ECPA), namely requests for subscriber information (18 U.S.C. § 2703(c)(1)) and for the content of emails more than 180 days old (18 U.S.C. § 2703(b)). In the latter case, however, the individual concerned has to be notified and thus has the opportunity to challenge the request in court. See *Bignami*, The U.S. legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens, p.18.

[135] According to the representations by the U.S. government, recipients of administrative subpoenas may challenge them in court on the grounds that they are unreasonable, i.e. overboard, oppressive of burdensome. See DOJ Representations (Annex VII), p. 2.

4. Adequate level of protection under the EU-U.S. Privacy Shield

(112) In the light of the those findings, the Commission considers that the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield.

(113) In particular, the Commission considers that the Privacy Principles issued by the U.S. Department of Commerce as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the basic principles laid down in Directive 95/46.

(114) In addition, the effective application of the Privacy Principles is guaranteed by the transparency obligations and the administration of the Privacy Shield by the Department of Commerce.

(115) Moreover, the Commission considers that, taken as a whole, the oversight and recourse mechanisms provided for by the Privacy Shield enable infringements of the Privacy Principles by Privacy Shield organisations to be identified and punished in practice and offer legal remedies to the data subject to gain access to personal data relating to him and, eventually, to obtain the rectification or erasure of such data.

(116) Finally, on the basis of the available information about the U.S. legal order, including the representations and assurances from the U.S. government, the Commission considers that any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Privacy Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference. The Commission concludes that this meets the standards of Article 25 of Directive 95/46/EC, interpreted in light of the Charter of Fundamental Rights of the European Union, as explained by the Court of Justice in particular in the *Schrems* judgment.

5. Action of Data Protection Authorities and information to the Commission

(117) In the *Schrems* judgment, the Court of Justice clarified that the Commission has no competence to restrict the powers that DPAs derive from Article 28 of Directive 95/46 (including the power to suspend data transfers) where a person, in bringing a claim under that provision, calls into question the compatibility of a Commission adequacy decision with the protection of the fundamental right to privacy and data protection.[136]

(118) In order to effectively monitor the functioning of the Privacy Shield, the Commission should be informed by Member States about relevant action undertaken by DPAs.

(119) The Court of Justice furthermore considered that, in line with the second subparagraph of Article 25(6) of Directive 95/46, Member States and their organs must take the measures necessary to comply with acts of the Union institutions, as the latter are in principle presumed to be lawful and accordingly produce legal effects until such time

[136] *Schrems*, paragraphs 40 et seq., 101-103.

as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality. Consequently, a Commission adequacy decision adopted pursuant to Article 25(6) of Directive 95/46 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities.[137] Where such an authority has received a complaint putting in question the compliance of a Commission adequacy decision with the protection of the fundamental right to privacy and data protection and considers the objections advanced to be well founded, national law must provide it with a legal remedy to put those objections before a national court which, in case of doubts, must stay proceedings and make a reference for a preliminary ruling to the Court of Justice.[138]

6. Periodic review of adequacy finding

(120) In the light of the fact that the level of protection afforded by the U.S. legal order may be liable to change, the Commission, following adoption of this decision, will check periodically whether the finding relating to the adequacy of the level of protection ensured by the EU-U.S. Privacy Shield is still factually and legally justified. Such a check is required, in any event, when the Commission acquires any information giving rise to a justified doubt in that regard.[139]

(121) Therefore, the Commission will continuously monitor the overall framework for the transfer of personal data created by the EU-U.S. Privacy Shield as well as compliance by U.S. authorities with the representations and commitments contained in the documents attached to this decision. Moreover, this decision will be subject to an Annual Joint Review which will cover all aspects of the functioning of the EU-U.S. Privacy Shield, including the operation of the national security and law enforcement exceptions to the Privacy Principles.

(122) To perform the Annual Joint Review referred to in Annexes I, II and VI, the Commission will meet with the Department of Commerce and FTC, accompanied, if appropriate, by other departments and agencies involved in the implementation of the Privacy Shield arrangements, as well as, for matters pertaining to national security, representatives of the ODNI, other Intelligence Community elements and the Ombudsperson. The participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party.

(123) In the framework of the Annual Joint Review, the Commission will request that the Department of Commerce provides comprehensive information on all relevant aspects of the functioning of the EU-U.S. Privacy Shield, including referrals received by the Department of Commerce from DPAs and the results of *ex officio* compliance reviews. The Commission will also seek explanations concerning any questions or matters concerning the EU-U.S. Privacy Shield and its operation arising from any information available, including transparency reports allowed under the USA FREEDOM Act, public reports by U.S. national intelligence authorities, the DPAs, privacy groups, media reports, or any other possible source. Moreover, in order to facilitate the Commission's task in this regard, the Member States should inform the Commission of

[137] *Schrems*, paragraphs 51, 52 and 62.
[138] *Schrems*, paragraph 65.
[139] *Schrems*, paragraph 76.

cases where the actions of bodies responsible for ensuring compliance with the Privacy Principles in the United States fail to secure compliance and of any indications that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection.

(124) On the basis of the annual joint review, the Commission will prepare a public report to be submitted to the European Parliament and the Council.

7. Suspension of the adequacy decision

(125) Where, on the basis of the checks or of any other information available, the Commission concludes that there are clear indications that effective compliance with the Privacy Principles in the United States might no longer be ensured, or that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection, it will inform the Department of Commerce thereof and request that appropriate measures are taken to swiftly address any potential non-compliance with the Privacy Principles within a specified, reasonable timeframe. If, after the expiration of the specified timeframe, the U.S. authorities fail to demonstrate satisfactorily that the EU-U.S. Privacy Shield continues to guarantee effective compliance and an adequate level of protection, the Commission will initiate the procedure leading to the partial or complete suspension or repeal of this decision.[140] Alternatively, the Commission may propose to amend this decision, for instance by limiting the scope of the adequacy finding only to data transfers subject to additional conditions.

(126) In particular, the Commission will initiate the procedure for suspension or repeal in case of:

(a) indications that the U.S. authorities do not comply with the representations and commitments contained in the documents annexed to this decision, including as regards the conditions and limitations for access by U.S. public authorities for law enforcement, national security and other public interest purposes to personal data transferred under the Privacy Shield;

(b) failure to effectively address complaints by EU data subjects; in this respect, the Commission will take into account all circumstances having an impact on the possibility for EU data subjects to have their rights enforced, including, in particular, the voluntary commitment by self-certified U.S. companies to cooperate with the DPAs and follow their advice; or

(c) failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects.

[140] As of the date of application of the General Data Protection Regulation, the Commission will make use of its powers to adopt, on duly justified imperative grounds of urgency, an implementing act suspending the present decision which shall apply immediately without its prior submission to the relevant comitology committee and shall remain in force for a period not exceeding six months

(127) The Commission will also consider to initiate the procedure leading to the amendment, suspension, or repeal of this decision if, in the context of the Annual Joint Review of the functioning of the EU-U.S. Privacy Shield or otherwise, the Department of Commerce or other departments or agencies involved in the implementation of the Privacy Shield, or, for matters pertaining to national security, representatives of the U.S. Intelligence Community or the Ombudsperson, fail to provide information or clarifications necessary for the assessment of compliance with the Privacy Principles, the effectiveness of complaint handling procedures, or any lowering of the required level of protection as a consequence of actions by U.S. national intelligence authorities, in particular as a consequence of the collection and/or access to personal data that is not limited to what is strictly necessary and proportionate. In this respect, the Commission will take into account the extent to which the relevant information can be obtained from other sources, including through reports from self-certified U.S. companies as allowed under the USA FREEDOM Act.

(128) [The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46 has delivered a favourable opinion on the adequate level of protection provided by the United States for personal data transferred under the EU-U.S. Privacy Shield from the European Union to self-certified organisations in the United States[141], which has been taken into account in the preparation of this Decision.]

(129) [The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31(1) of Directive 95/46[142],]

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.

2. The EU-U.S. Privacy Shield is constituted by the Privacy Principles issued by the U.S. Department of Commerce on [Date] as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I, III to VII.

3. For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the "Privacy Shield List", maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Privacy Principles set out in Annex II.

---

141 [Reference]
142 [Reference]

Article 2

This Decision does not affect the application of the provisions of Directive 95/46/EC other than Article 25(1) that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

Article 3

Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive 95/46/EC leading to the suspension or definitive ban of data flows to an organisation in the United States that is included in the Privacy Shield List in accordance with Sections I and III of the Privacy Principles set out in Annex II in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall inform the Commission without delay.

Article 4

1. The Commission will continuously monitor the functioning of the EU-U.S. Privacy Shield with a view to assessing whether the United States continues to ensure an adequate level of protection of personal data transferred thereunder from the Union to organisations in the United States.

2. The Member States and the Commission shall inform each other of cases where it appears that the government bodies in the United States with the statutory power to enforce compliance with the Privacy Principles set out in Annex II fail to provide effective detection and supervision mechanisms enabling infringements of the Privacy Principles to be identified and punished in practice.

3. The Member States and the Commission shall inform each other of any indications that the interferences by U.S. public authorities responsible for national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go beyond what is strictly necessary, and/or that there is no effective legal protection against such interferences.

4. Within one year from the date of the notification of this Decision to the Member States and on a yearly basis thereafter, the Commission will evaluate the finding in Article 1(1) on the basis of all available information, including the information received as part of the Annual Joint Review referred to in Annexes I, II and VI.

5. The Commission will report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC.

6. The Commission will present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC with a view to suspending, amending or repealing this Decision or limiting its scope, among others, where there are indications:

– that the U.S. public authorities do not comply with the representations and commitments contained in the documents annexed to this Decision, including as regards the conditions

and limitations for access by U.S. public authorities for law enforcement, national security and other public interest purposes to personal data transferred under the EU-U.S. Privacy Shield;

– of a systematic failure to effectively address complaints by EU data subjects; or

– of a systematic failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects in accordance with his functions as set out in Annex III.

The Commission will also present such draft measures if the lack of cooperation of the bodies involved in ensuring the functioning of the EU-U.S. Privacy Shield in the United States prevents the Commission from determining whether the finding in Article 1(1) is affected.

Article 5

Member States shall take all the measures necessary to comply with this Decision.

Article 6

This Decision is addressed to the Member States.

Done at Brussels,

For the Commission
[…]

Member of the Commission

ANNEXES

ANNEX I: Letter from U.S. Secretary of Commerce Penny Pritzker
Annex 1: Letter from Under Secretary for International Trade Stefan Selig
ANNEX II: EU-U.S. Privacy Shield Principles
Annex I: Arbitral Model
ANNEX III: Letter from U.S. Secretary of State John Kerry
Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism
ANNEX IV: Letter from Federal Trade Commission Chairwoman Edith Ramirez
ANNEX V: Letter from U.S. Secretary of Transportation Anthony Foxx
ANNEX VI: Letter from General Counsel Robert Litt, Office of the Director of National Intelligence
ANNEX VII: Letter from Deputy Assistant Attorney General Bruce Swartz, U.S. Department of Justice